ZENO B. BAUCUS
Assistant U.S. Attorney
U.S. Attorney's Office
James F. Battin U.S. Courthouse
2601 Second Avenue North, Suite 3200
Billings, MT 59101
Phone: (406) 657-6101
FAX: (406) 657-6989
Email: zeno.baucus@usdoj.gov

ATTORNEY FOR PLAINTIFF
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BILLINGS DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH: **FACEBOOK USER tyler.emineth.397**	**MJ-18-37-BLG-TJC** **BRIEF IN RESPONSE TO COURT'S JULY 30, 2018, ORDER**

The United States hereby submits this memorandum in response to the Court's inquiry concerning the method of examination that law enforcement will employ in reviewing the returns associated with the instant search warrant. The memorandum also seeks to address any legal or practical issues associated with the review.

PROCEDURAL BACKGROUND

On June 21, 2018, Tyler Emineth was indicated on three counts relating to the Production of Child Pornography, in violation of 18 U.S.C. § 2251(a). Doc. 1. On July 26, 2018, the government submitted an application for a search warrant, search warrant, and supporting affidavit to the Court in connection with the search of the account associated with Facebook user tyler.emineth.397 ("Facebook Warrant"). As detailed in the supporting affidavit, the Facebook Warrant disclosed facts that indicated that account had been used to solicit and produce child pornography. The warrant directed Facebook to produce certain specific information associated with that account, as identified in Attachment B.I to the affidavit. From that information, the warrant then permitted the government to seize information pertaining to five categories of data relating to child pornography, including usage information. *See* Attachment B.II.

Moreover, the affidavit to the Facebook Warrant contained the procedures that the government would following in reviewing the collected data. As cited by their corresponding paragraphs in the affidavit, those procedures included the following:

> 56. The initial examination of the electronic information will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the

time period from the Court within the original 120-day period from the date of execution of the warrant.

57. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders responsive to this search warrant do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

58. If an examination is conducted, and the electronic information produced in response to this warrant does not contain any data falling within the ambit of the warrant, the government will seal any non-responsive information, absent further authorization from the Court.

59. The government will retain a forensic image of all of the electronic information produced in response to this warrant for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

On July 30, 2018, in response to the submission of the Facebook Warrant, this Court issued an order directing the United States to submit a brief "addressing (1) whether the [Facebook Warrant]...complies with the Ninth Circuit's recommendations in *CDT* or *Flores*; and if not, (2) why this Court can and should disregard the Ninth Circuit's recommendations." July 30, 2018, Order at 3 (the "Order"). This briefing responds to the Order.

ARGUMENT

A search warrant complies with the Fourth Amendment when it includes three elements: it must be issued by a neutral magistrate; it must satisfy the particularity requirement; and it must be based on a showing of "probable cause to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense." *Dalia v. United States*, 441 U.S. 238, 255-56 (1979). The scope of the particularity clause is limited to "two matters"—"the place to be searched and the persons or things to be seized." *United States v. Grubbs*, 547 U.S. 90, 97 (2006). In particular, "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that search warrants also must include a specification of the precise manner in which they are to be executed." *Id.* at 98 (quoting *Dalia*, 441 U.S. at 255).

The search warrant here includes these three elements. First, this Court is a neutral magistrate authorized to issue the warrant by 18 U.S.C. §§ 2703 and 2711(3). Second, the search warrant specifies with particularity the place to be searched and things to be seized. Attachment A identifies with particularity the place to be searched, the targeted Facebook account. Attachment B.II, the "[i]nformation to be seized by the government," identifies with particularity the items to be seized; it is limited to particular categories of records that constitute

evidence, fruits, contraband, or instrumentalities of the specified crimes. *See, e.g.*, *United States v. Kuc*, 737 F.3d 129, 132-33 (1st Cir. 2013); *United States v. Adjani*, 452 F.3d 1140, 1148-49 (9th Cir. 2006) (holding that computer warrant with similar formulation to this warrant satisfied particularity clause). Third, the affidavit establishes probable cause to believe that information located in the place described in Attachment A and identified in Attachment B.II will constitute evidence, contraband, fruits, or instrumentalities of the specified crimes. Under *Dalia* and *Grubbs*, these are the only elements required for a warrant to satisfy the Fourth Amendment.

Citing *United States v. Comprehensive Drug testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) ("*CDT*"), and *United States v. Flores*, 802 F.3d 1028 (9th Cir. 2015), the Order discusses certain steps that the Ninth Circuit has recommended in the context of search warrants. Order at 1-2. The "guidance" proposed by the concurring opinion in *CDT* is meant to offer the "government a safe harbor" that, should they later be challenged, a warrant will be "deemed reasonable and lawful." *CDT*, 621 F.3d at 1178. The Facebook Warrant complies with *CDT* and *Flores* and is proper pursuant to the Fourth Amendment.

I. The Facebook Warrant proposes a two-step review consistent with *CDT* and *Flores*.

Rule 41 of the Federal Rules of Criminal Procedure explicitly authorizes the two-step procedure for warrants for electronic evidence. Rule 41(e)(2)(B) specifies that a warrant may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. Fed. R. Crim. P. 41(e)(2)(B).[1] This fact makes the two-step procedure for warrants for electronic evidence reasonable under the Fourth Amendment.

As noted in the Order, however, *Flores* and *CDT* endorse a two-step review process whereby law enforcement (1) seized and conducted an initial review of the subject Facebook account and (2) segregated information that was nonresponsive and sealed that information, absent an order from the Court. Order at 3 (*quoting United States v. Brady*, 2016 WL 8856696, *8 (D. Or. Sept. 14, 2016)).

---

1 The Advisory Committee Notes explain that the two-step process is "inherent in searches for electronically stored information." Fed. R. Crim. P. 41, Advisory Committee's Notes (2009 amend.). The Notes recognize that electronic storage media "commonly contain such large amounts of information that is often impractical for law enforcement to review all of the information during execution of the warrant at the search location." *Id.*

The Facebook Warrant proposes those exact steps here. As addressed in Attachment B.I to the Facebook Warrant, Facebook would be required to produce certain information associated with the tyler.eminth.397 account to the government.[2] The government, pursuant to B.II, would then review that information for responsive data to the warrant. The responsiveness of that information would turn on whether that material related to any one of the four categories of matters cited in B.II. These procedures would encapsulate the two steps contemplated by Rule 41(e)(2)(B) and supporting case law. *See e.g.*, *Flores*, 802 F.3d at 1028 (upholding warrant that authorized investigators to search entire Facebook account for specified evidence); *United States v.* Hay, 231 F.3d 630, 637-39 (9th Cir. 2000) (holding that officers were justified in removing computers for off-site search "because of the time, expertise, and controlled environment required for a proper analysis:); *United States v. Hill*, 322 F. Supp 2d 1081 (C.D. Cal. 2004) (police not required to limit search to those files (or filenames) that seem most likely to be associated with child pornography, such as those with ".jpg" suffixes or those containing the word "sex"); *In the Matter of A Warrant for*

---

2 Attachment B.II provides that the government may only pull relevant information "since April 29, 2018." As noted in the accompany affidavit, this is the date that the subject Facebook account was created and was subsequently utilized to solicit additional child pornography in June 2018, prior to Emineth's arrest. *See* Affidavit, ¶¶30,36. This temporal limitation provides an additional safeguard that the warrant approved in *Flores* did not. *Flores*, 802 F.3d at 1045.

All Content and Other Information Associated with the Email Account xxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) (holding that case law concerning searches of hard drives and other storage media supports the government's ability to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant); *cf. United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006) (holding that restricting computer search to specific search terms "would likely have failed to cast a sufficiently wide net to capture the evidence sought.").

Then, as noted above and considered by the Order, the government would segregate data that was initially reviewed and found to be non-responsive and would not subsequently access that data absent authorization from the Court. *See* Affidavit, ¶ 60.[3] Such an approach would be consistent with the "second" step outlined by the Order.[4]

---

3 Based on previous productions of data by Facebook, the production here would likely take the form of a single pdf document. Per discussions with the investigative team, the initial review would entail going through that document and "cutting out" individual pages that were nonresponsive. While burdensome, the investigative team has indicated that is the process that will be employed here.

4 The United States respectfully submits that even the absence of this protocol would not be fatal to the warrant. *See United States v. Schesso*, 730 F.3d 1040, 1043 (9th Cir. 2013) (Reversing motion to suppress, in part, on the grounds that a search warrant that called for the collection of electronic evidence from a residence

II. The Use of a Filter Team is Unnecessary and Unworkable

The Order construes a footnote from *Flores* as a recommendation that, if possible, investigative agents not be involved in the initial review of the totality of data produced by Facebook. Order at 3. As quoted by the Order, the *Flores* court stated that "[i]deally, the government's investigative team would not have been involved in segregating responsive data…" Order at 3. The Court "construes this as a recommendation that the investigative agents not be involved" in the initial review. *Id.* (citing *CDT*, 621 F.3d at 1168, 1172). However, that same passage in *Flores* also noted that "*CDT* did not prohibit investigative teams from participating in data segregation as a general matter, however, and instead faulted the government for misleadingly suggesting in the warrant that the team would not be involved. *CDT* thus serves as a reminder not to mislead magistrates

---

and did not contain search protocols was permissible because the concerns raised by *CDT* were not present); *United States v. Hernandez*, 2016 WL 471943, *4, (S.D.Cal. Feb. 8, 2016) (rejecting defendant's argument that "'the government should have provided the court methods and procedures it would use to look in limited areas of the phone for limited information."); *United States v. Russian*, 2017 WL 676501 (10th Cir. Feb. 21, 2017) ("But we note, like other circuits, we have previously declined to require a search protocol for computer searches, since courts are better able to assess the reasonableness of search protocols ex post…"); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1260-71 (2010) (noting that Supreme Court precedent "point[s] to the conclusion that the Fourth Amendment does not permit ex ante restrictions on the execution of computer warrants.").

or exceed the scope of a warrant, not as a blanket prohibition on data segregation by investigative teams." *Flores*, 802 F.3d at 1045 n. 22. Moreover, *Flores* statement cites to a passage in *CDT* addressing concerns regarding third-party data, which *Flores* makes clear was not issue in that case. *See Flores*, 802 F.3d at 1045. For the following reasons, the United States respectfully submits that, unless certain concerns are implicated, the use of a so-called filter team is unnecessary and unworkable.

A. The use of a taint or filter team is only necessary in highly fact specific cases where the presence of third party data creates a clear risk that third party information will be compromised.

It is important to distinguish between two different kinds of "over-seizing" that stem from electronic searching, and the particular harm from which a filter team provides protection.

As courts have recognized, "'over-seizing' is an accepted reality in electronic searching because there is no way to be sure exactly what an electronic file contains without somehow examining its contents.'" *Flores*, 802 F.3d at 1044 (citation omitted). This reality is present even when the electronic searching involves only a single individual's information, and requires the protections described in the previous section in order "to prevent necessary 'over-seizing' from turning into a general dragnet." *Id.* In particular, the requirement that the

warrant specify the particular crime with limits on retaining nonresponsive data under the "plain view" doctrine further guards against concerns involving over-seizing.

With respect to these protections, however, the identity of the reviewing agent is immaterial. The reviewing agent, whether part of the investigative team or not, would necessarily need enough information about the crime being investigated to sort responsive information from nonresponsive. And evidence that truly falls into the "plain view" doctrine, *i.e.*, evidence immediately apparent during the review as evidence of a crime outside the one being investigated (such as opening a file revealing child pornography on a computer being investigated for evidence of wire fraud), necessarily would trigger the same alarm whether the reviewer is part of the original investigation or not. A filter team provides no extra protections in this respect.

There are specific kinds of data, however, where there is a particular risk when the review is conducted by the investigative team. That is the risk that the review may reveal information that *is* responsive to the original investigation, but which the investigators are not entitled to see, either because it involves third parties' rights or because the information is subject to some sort of privilege.

In cases, like *CDT*, where the data to be reviewed necessarily covers third-party data for which no probable cause exists, the risk is not simply the invasion of privacy of third parties generally or the risks of uncovering some sort of criminal activity without probable cause. These harms that are identical regardless of the agent. Instead, the particular risk posed from review by the investigating agents is uncovering evidence about the crime being investigated (information that is, in that respect, responsive) but which is outside of the warrant because there was not probable cause to search the third party's data but for the fact that it was intermingled. Similarly, in a review of potentially attorney-client information or medically privileged information, a filter team is not needed because of the general invasion of privacy (which, again, would be the same for any agent) but because of the risk investigators viewing responsive but privileged information that they would not be able to un-see. Any discussion of filter teams must stem from situations, such as these, where the particular harm to be addressed calls for the particular remedy of a filter team.

There are certainly situations where a taint or filter team should be part of a warrant. Nevertheless, these situations are limited to those where the protection of the filter team matches the risk of reviewing third-party or privileged information. In *CDT* the United States had probable cause to search for and seize

drug testing information from ten specific individuals. *Id.* at 1166. This information was maintained at a drug testing facility where the information regarding the ten individuals was intermingled with the private information of countless other individuals that the United States did not have probable cause to search or seize.[5] *Id.* The warrant authorized the seizure and the search of any data system that might contain the information regarding the ten individuals. *Id.* at 1168.

Recognizing that this seizure would expose and violate the privacy of all the third parties whose data was also stored on the system, the warrant required that a filter team separate the relevant data regarding the ten individuals from the data of third parties. *Id.* at 1168-1169. Unfortunately, the United States ignored this limitation and, under a theory of plan view, attempted to retain the data of many of the third parties who may have been incriminated during the review of the data systems. *Id.* at 1169-1170.

Eventually, the Ninth Circuit intervened and prevented the United States from retaining this information. In doing so, it affirmed that a taint or filter team

---

5 It is worth noting that this information would normally be subject to a subpoena asking for only the files of those individuals. Unfortunately, because of the risk of spoliation in that case, CDT was not trusted to turn over the responsive information, requiring a more invasive seizure.

may sometimes be necessary when the United States seeks a warrant to seize a large electronic database where there is a clear possibility that the relevant records of a suspect might be intermingled with the private data of third parties for whom the United States does not have any probable cause to suspect any wrongdoing. As the Court explained,

> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect. *Id.* at 1177.

CDT is a sensible framework for how to proceed in rare circumstances requiring seizure of a large amount of third party data. Nevertheless, the search protocols it suggests should not be used in every case, particularly those involving a single individual's electronic device or account. They should be reserved specifically to instances when the government must conduct an initial review to segregate extraneous, third party data which it does not independently have probable cause to seize and/or has concerns that any privileges may be implicated.

Indeed, the proper use of a taint team is a highly fact specific determination. There should not be a generalized requirement to use them because they are only

useful in very specific circumstances where the government is seeking a broad warrant to seize a database where the data of suspects and third parties are intermingled and such data will, consequently, come under examination even though the United States does not have probable cause to review such information.

This is particularly true when the seizure is of a single individual's electronic device or account. The Ninth Circuit clarified this exact point in a *United States v. Schesso*, 730 F.3d 1040 (9th Cir. 2013). In that case, a defendant accused of possessing and manufacturing child pornography challenged the validity of a warrant because the warrant issued by a state judge had not created a search protocol and taint team like the one the government failed to abide by in *CDT* *Id.* at 1047. The Ninth Circuit unequivocally rejected the defendant's argument. As the court explained, "Tellingly, the search did not involve an over-seizure of data that could expose sensitive information about other individuals not implicated in any criminal activity—a key concern in both the per curiam and concurring opinions of *CDT []*—nor did it expose sensitive information about Schesso other than his possession of and dealing in child pornography." *Id.* at 1047-1048.

There is a key distinction between *Schesso* and *CDT* that must be remembered when considering the necessity of a taint team. That distinction is

the nature of the seizure. If the government is seeking a warrant which requests the seizure of a large database or electronic storage system that contains both information about a suspect that is supported by probable cause and information on third parties for which the government does not have probable cause, the utilization of a filter team may be necessary. However, and as is the case here and with respect to most search warrants pertaining to electronic evidence, if the government is seeking a limited warrant for the data of one individual and the search does not necessitate the inspection of third party data, a filter team is not required.

Here, the Facebook Warrant has requested the data regarding one specific user and has not requested authority to seize and search a broader database to locate those records among third party data. At no time will the government be empowered to seize and search thorough the records of other users' accounts. Facebook will be responsible for segregating the user's information and will only provide information from that account. There is no chance that an innocent third party's account will be disclosed and the United States is not seeking permission to comb thorough third party data. *See Flores*, 802 F.3d at 1045 ("Facebook, rather than government agents, segregated Flores's account to protect third parties' rights."). As a result, there is no need for a taint or filter team. This is

essentially the same as the search approved in *Schesso* and *Flores*. It is only the data of one user, and that data is firmly supported by probable cause.[6]

B. *United States v. Flores* and *United States v. Bundy* do not require the use of a taint or filter team.

Both *United States v. Flores* 802 F.3d 1028 (9th Cir. 2015) and *United State v. Bundy*, 195 F.Supp.3d 1170 (9th Cir. 2016) address, in passing, the use of filter teams and do not alter the instant analysis. A taint team or officer was not used in either case and while the Order construes *Flores* for the proposition that a filer team is recommended, the United States respectfully submits that such a procedure is generally not necessary or reasonable.

In *Bundy*, the Court stated "Although the use of a filter team separate from the investigation team to conduct the initial review would have been an added layer of protection for ensuring the investigation team did not benefit from exposure to information that was not responsive to the Warrant, there is not any such requirement in the Warrant nor does the *Flores* court require such an additional safeguard." *Bundy*, 195 F.Supp.3d at 1176. A taint or filter team is explicitly

---

6 Indeed, a grand jury has made a probable cause finding that Eminth produced child pornography and, on August 1, 2018, Eminth notified the Court that he intends to enter a plea of guilty. Doc. 17. Based upon a showing of probable cause, the Facebook Warrant merely seeks evidence, and ultimately the identities of other victims, for purposes of notifying those victims and holding Emineth accountable for the totality of his actions.

excepted from the requirements laid out by these cases. While such a team add an additional layer of protection with respect to specific risks, it is not appropriate or feasible to do this in every case. As shall be discussed below, the federal investigatory agencies in Montana do not have the staff or resources to create a taint team or agent in every case where this sort of information is sought. As such, the United States does not believe that instituting a taint team requirement is necessary or feasible in most cases.

Moreover, other District Courts have held that there are instances when the requirement of a filter team is not appropriate. The United States has enclosed *United States v. Sealed Warrant*, one such example of this.[7] In that order, the district court concluded that it was not appropriate to force the government to use a filter team when they had received a warrant based on probable cause to seize and review a single email account.

C. **Routine use of a taint or filter team would be logistically impossible and significantly hamper Investigations.**

The United States believes that routinely requiring a taint team would critically strain the resources of these agencies. Given the relatively small personnel size of most of these agencies in Montana, it is simply impossible and

7 That Memorandum and Order, issued by United States District Judge Hopkins from the Northern District of Alabama, is attached as Exhibit A.

unrealistic to have an agent walled off and unable to participate in every case where a warrant of this kind is requested.

Because these offices are small, most investigations are done collaboratively. One agent may be the main case agent, but duties including surveillance, records review, and undercover operations are shared by most of the members of an office. In special cases where a *CDT* type of seizure is present, they can accommodate, but creating a taint team is something they cannot logistically do with respect to every individual electronic device or account at issue.

Every agent who is conflicted out due to taint team duties, is a significant loss to an investigation. When such a team is not require by case law, the United States believes it would be an unfair and unnecessary burden to require the formation of such a team. Additionally, due to the use of codes, aliases, burner phones, and other efforts to hide illegal activity, an agent separated from the investigation may be unable to separate the relevant data from the irrelevant data without proper knowledge and context of the case. See *United States v. Adjani*, 452 F.3d 1140, 1149-1150 (9th Cir. 2006). Messages that might appear innocuous to someone without knowledge of the case could actually be crucial evidence (whether inculpatory or exculpatory) of the crimes at issue. In order to

properly interpret the significance of a document or other information that may relate to a criminal enterprise, investigators may need to know all about the participants and the practices of the enterprise. Furthermore, segregation of responsive from non-responsive information is typically a dynamic process; information learned during segregation may affect judgments regarding whether other information falls within the scope of the warrant. Thus, at a minimum, prior to the filter team beginning work, members of the investigative team will need to spend substantial efforts educating members of the filter team about the case, and members of the filter team must spend time learning it. These procedures would significantly increase the costs of conducting investigations, and additional appropriate personnel may not always be available to participate. Even when they are, members of the filter team are unlikely to know the case as well as members of the investigate team, so some responsive information may not be recognized and passed to the investigative team.

III. Conclusion

The United States is mindful of the Court's desire to vigilantly protect the privacy interests of innocent third parties and the United States supports that notion. Indeed, constitutional requirements aside, the United States support the procedural safeguards proposed by the Facebook Warrant. The utilization of a

two-step review process and the segregation of non-responsive information adequately protects any privacy interests while permitting law enforcement to search for evidence relating to the production of child pornography, upon a showing of probable cause. However, because of the logistical cost of creating taint and filter teams, the United States requests that the Court only require them in those cases that implicate the concerns addressed in *CDT* This will maintain the important goal of protecting third party data while still enabling Federal Law Enforcement Agencies to effectively investigate criminal cases. The United States respectfully submits that the Facebook Warrant effectively strikes this balance.

DATED this 6th day of August, 2018.

KURT G. ALME
United States Attorney

ZENO B. BAUCUS
Assistant U. S. Attorney

CERTIFICATE OF COMPLIANCE

Pursuant to D. Mont. L.R. 7.1(d)(2) and CR 47.2, the attached Response to Court's July 30, 2018 Order is proportionately spaced, has a typeface of 14 points or more, and the body contains 4,211 words.

ZENO B. BAUCUS
Assistant U. S. Attorney

FILED
2017 Aug-08 PM 04:46
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
v.	)	**Case No.: 2:17-CR-103-VEH-TMP-1**
	)	
SEALED SEARCH WARRANT,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Pending before this court is the Government's Motion To Review Order Requiring Government To Use Filter Team for Search Warrant (hereinafter "Motion To Review"). The Government seeks to have the magistrate judge's Order requiring it to use a filter team[1] when executing a search warrant (hereinafter "Filter Team Order") vacated. For the reasons set out below, the Motion will be granted and the Filter Team Order will be vacated.

The Supreme Court has found that a district court may "review [in] whole," "[review] in part anew," or "wholly ignore" a magistrate judge's order. *Mathews v. Weber*, 423 U.S. 261, 263 (1976). "The authority to make an informed, final determination, [the Supreme Court] emphasize[s], remains with the [district] judge" *Id.* at 271. The district court retains total control and jurisdiction over "the entire

---

[1] Defined and discussed *infra* beginning at page 4.

process." *United States v. Raddatz* 447 U.S. 667, 681 (1980); *see also Webb v. Califano*, 468 F.Supp. 825, 830 (E.D. Cal. 1979) ("[T]he district court *must* give a de novo review when timely objections are filed, and the court *may* give whatever review it deems appropriate, in its discretion, when no objections are filed." (emphasis added)).

This court has exercised its discretion to conduct a *de novo* review of the magistrate judge's order and the underlying search warrant.

I. Background[2]

On February 6, 2017, the Government applied for a warrant to search an email account that has been used to defraud people in multiple states over several years. The owner of the account is currently unknown and one of the goals of the warrant is to identify any persons using the account to commit the crimes being investigated. The warrant sought would allow the Government to search all messages in the account within the stipulated date range. The date range sought started six months before the first known theft and ran to the date of the warrant application. The application provided for a "two-step process"[3] in executing the search. Beyond describing that process, the Government did not specify what

[2] Citations to the record have been omitted because the record is sealed.

[3] Defined and discussed *infra* beginning at page 5.

strategy it intended to use to search the information surrendered by the email service provider.

At 2:10 PM on February 6, 2017, the magistrate judge signed and issued the warrant to search the email account. At 4:57 PM, the magistrate judge issued the Filter Team Order because he felt the breadth of the information sought necessitated greater privacy protection than is usually afforded in a search. The Filter Team Order required the Government to use a filter team to limit the scope of the material reviewed by the investigators to evidence "reasonably identifiable as relevant to the investigation." The Government filed a Motion To Reconsider the Filter Team Order (hereinafter "Motion To Reconsider") on February 21, 2017. The Government sought to have the Filter Team Order vacated. The magistrate judge entered an Order (hereinafter "Reconsideration Order") denying the Motion To Reconsider. The Government then filed the Motion To Review with this court. Neither the magistrate judge nor the Government has indicated that there is reason to believe there is privileged information in the email account.

While the Government has not divulged its exact search strategy, the process that is likely to be used is not as Orwellian as the magistrate judge seems to fear. During a computer search, the Government agents generally do not manually search each and every document that is present on the drive. Undertaking a search of that

nature is far too laborious to prove helpful in an investigation because it could take up to twenty-eight man-years to read all of the text that could be stored in the targeted account.[4] Since this is plainly an unworkable time frame for a criminal investigation, the Government will most likely use keyword searches using forensic software to attempt to locate incriminating information in the files. Only after this process occurs will the information be reviewed by a human agent and a determination made about whether it falls within the scope of the warrant. In essence, the Government's software is already acting as a "filter" to protect innocuous information from investigators, and only potentially relevant items will be reviewed by Government agents.

A. Filter Teams

A "filter team," also called a "taint team," refers to a search procedure in which the team executing a search is divided into two groups: an investigative team and a filter team. The filter team is the group that actually searches the material obtained pursuant to the warrant. During the search, the filter team identifies files responsive to the warrant and passes only those files on to the investigative team.

---

[4] The email account in question can store at least 15 gigabytes of information. This amount can be expanded for a fee. A free account would be able to store 15 billion characters. Assuming an average word length of 4.5 characters, the account can hold 3.3 billion words. Assuming the investigator can read 225 words per minute, the investigator will need 14,814,815 minutes, or 28 years, to read all of the text in the account.

This process creates an "ethical wall"[5] by separating the investigative team from information not relevant to the alleged criminal activity which supported the issuance of the warrant.

Traditionally, filter teams have been used to protect privileged information, such as documents from a doctor's, lawyer's, or congressman's office, from being viewed by investigators.[6] In the present case, the magistrate judge ordered the Government to use a filter team to prevent investigators from viewing any innocuous files intermingled with responsive files. More specifically, the order was not limited to files containing privileged information.

B. Two-Step Search Process

The Government intends to use a two-step search process in executing the warrant. In the first step, all files the Government has probable cause to believe might contain evidence of the crime are copied and seized by the Government. In the second step, the Government searches all the files it has seized to identify which

---

[5] This was sometimes called a "Chinese wall" in the past, but the term is now disfavored by some courts due to its ethnic derivation.

[6] For example, a Westlaw search using the keywords "filter team" (including quotation marks) returns fifty-two cases which include the phrase. In forty-three of those cases the Government elected to use filter teams because it had reason to believe that the documents being searched included privileged information. The Westlaw search only returned two cases where a magistrate judge required the Government to use filter teams against the Government's wishes. In both of those cases, the district judge found the filter team requirement contrary to law. (discussed *infra* at 14, 15.) (The other seven cases are irrelevant to this discussion).

files are responsive to the warrant. The responsive files are retained by the investigators and the non-responsive files are sealed. This process is permitted by FED. R. CRIM. P. 41(e)(2)(B). By inserting the filter team between steps one and two, the magistrate judge's order has essentially created a three-step process.

II. Validity of the Search Warrant

Before addressing the validity of the Filter Team Order, this court must determine whether the warrant was valid. If the warrant was not valid, that is, if it failed to satisfy the requirements of the Fourth Amendment, then the Filter Team Order will not save the warrant.

The Supreme Court has interpreted the Fourth Amendment to "*only* require three things" in order for a warrant to be issued. *Dalia v. United States.*, 441 U.S. 238, 255 (1979) (emphasis added). (1) A search warrant must be issued by a neutral, disinterested magistrate; (2) the Government must demonstrate probable cause that the search will yield evidence, fruits of the crime, instrumentalities, or contraband; and (3) the warrant must particularly describe "the things to be seized as well as the place to be searched." *Id.*, 441 U.S. at 255 (internal quotes omitted). Beyond these three requirements, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general

Fourth Amendment protection against unreasonable searches and seizures." *Id.* at 257. Despite this deference shown to the Government, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 258.

"Probable cause exists when there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Grubbs*, 547 U.S. 90, 95 (2006). The Fourth Amendment "specifies *only* two matters that must be particularly described in the warrant: the place to be searched and the persons or things to be seized." *Id.* at 97 (emphasis added).

A warrant to search electronic communications may be issued by a "court of competent jurisdiction." 18 U.S.C. § 2703(a). A "court of competent jurisdiction" is defined in this chapter to include, *inter alia,* "any district court of the United States." 18 U.S.C. § 2711(3)(A). This court is a district court of the United States and it is therefore "a neutral, disinterested magistrate" empowered to issue warrants.

This court concurs with the magistrate judge's determination in the warrant that there is "a fair probability" that evidence of the crimes described in the Government's affidavit will be found in the targeted email account.[7] Therefore, the

[7] Specific discussion of the facts establishing probable cause has been omitted to protect the investigation.

Government has shown probable cause to search the files in the email account that were created between the dates the Government specified.

The particularity requirement of the Fourth Amendment was intended "to prevent general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). To avoid becoming a general search, the search must be limited to "specific areas and things for which there is probable cause to search." *Id.* As discussed above, the warrant has established probable cause to search the account in question and the warrant particularly describes the date range within the account to be searched. So, the Government has satisfied the particularity requirement vis-á-vis the search. However, the particularity requirement also requires the warrant to enable "the searcher to reasonably ascertain and identify the things authorized to be seized." *United States v. Bradley*, 644 F.3d 1213, 1259 (11th Cir. 2011). The Government met that standard. *See also United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006) (holding that a warrant with a similar formulation to the instant warrant satisfied the particularity requirement). Thus, the warrant satisfies the particularity requirement.

Since the warrant satisfies the three requirements set out by the Supreme Court in *Dalia*, the warrant is valid.

III. Analysis of the Filter Team Order

A. The Fourth Amendment Has Provided the Balance That Is To Be Weighed When Determining Whether a Warrant Should Be Issued and There Is "No Occasion" To Alter That Balance.

In the Filter Team Order, the magistrate judge stated that he was concerned that allowing the Government to execute the search without a filter team would violate the privacy rights of the account owner because, the magistrate judge argued, the two-step nature of the search process creates special privacy considerations. However, the Supreme Court has ruled that "probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness" are sufficient preconditions to a warrant to prevent unreasonable violations of privacy. *Zurcher,* 436 U.S. at 565. In *Zurcher*, the Court examined whether the fact that the target of a search warrant was a newspaper created special privacy considerations that required a re-balancing of the public and private interests that are weighed when issuing a warrant. *Id.* at 552. The newspaper argued that it was part of the press, and the First Amendment therefore afforded it greater privacy than the general public enjoyed. *Id.* at 552. The Court rejected the newspaper's argument and ruled that "the Fourth Amendment itself has struck the balance between privacy and public need, and there is no occasion or justification for a court to revise the amendment and strike a new balance." *Id.* at 559. In finding this, the

Supreme Court held that there is only one privacy standard: the standard set by the Fourth Amendment. Since there is only one privacy standard, electronically stored information (hereinafter "ESI") is not given more privacy protection than the accused's home, car, or any other property.

The magistrate judge cites two cases to support his view that the balancing test set out in the Fourth Amendment must be altered in light of the unique character of computer searches. Neither of the cases are binding on this court, nor does the court find them persuasive as to the issue presented in the Motion.

The first case, *United States v. Ganias*, is a Second Circuit case from which the magistrate judge quoted as follows: "Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools." *United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014). However, the question before the court in *Ganias* was whether "the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer." *Id.* at 137. The "modern, more sophisticated" approach that concerned the Second Circuit was the Government's ability to retain information indefinitely, not its ability to search the entire computer initially. That

court reasoned that, if the Government was allowed to indefinitely retain every file on the computer, then every document on the computer had been seized. The Government could search both the responsive and non-responsive documents repeatedly for crimes unrelated to the warrant. Therefore, the warrant was no longer particular, but in fact had become a general warrant. *Id.* In contradistinction to the facts of *Ganias*, in the present case, the Government has particularly described the files it intends to seize and there is no indication that the Government intends to keep the searched files indefinitely. Accordingly, *Ganias* does not address the issue before this court.

The second case that the magistrate judge cited was *United States v. Adjani.* In *Adjani*, the Ninth Circuit considered whether a search was too broad because the Government seized a computer that was not owned by the defendant but was located in his house. *United States v. Adjani*, 452 F.3d 1140, 1144 (9th Cir. 2006). This case actually cuts against the magistrate judge's argument, because the Ninth Circuit found that a search of the entire computer was reasonable despite the computer's not being owned by the defendant, while the current case only targets the account believed to have been used to commit the crimes alleged. *Id.* at 1148. The magistrate judge quoted the Ninth Circuit as follows, "The fact of an increasingly technological world is not lost upon us as we consider the proper

balance to strike between protecting an individual's right to privacy and ensuring that the [G]overnment is able to prosecute suspected criminals effectively." *Id.* at 1144. However, this is *dicta*. The *Adjani* court allowed the Government to execute the warrant in the case despite the "increasingly technological world." In essence, while the court explicitly acknowledged that a tremendous amount of information can be gathered by searching new technology, it held that a search of an entire computer is appropriate if probable cause can be shown to justify it. *Id.* at 1152; *see also In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) ("[T] he case law we have cited concerning searches of hard drives and other storage media supports the Government's ability to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant.").

The magistrate judge was correct that his role is "to balance the individual's privacy interest against the [G]overnment's need to detect crime." However, "to strike this balance by requiring a filter team" alters the balance that has been struck by the Fourth Amendment and explicated in *Zurcher*. Therefore, the Filter Team Order will be vacated.

B. The Government Is Permitted To Review Documents That May Be Non-Responsive to the Warrant To Determine Which Documents Are, in Fact, Responsive.

While the magistrate judge is likely correct that there are innocuous emails amongst any incriminating ones, "some perusal" is generally necessary to determine the "relevance of documents to the crime." *United States v. Slocum*, 708 F.2d 587, 604 (11th Cir. 1983); *see also Andresen v. Maryland* 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."). In noting that "an officer executing a warrant is entitled to examine any document he discovers" (*Slocum* at 604), the Eleventh Circuit has shown that it has contemplated the fact that officers executing a search of documents will inherently be exposed to documents and information that are not the subject of the warrant, but the Circuit does not consider such cursory review alone to be a violation of the Fourth Amendment. However, the Government's perusal must cease once the inapplicability of the warrant becomes clear. *Id.*

When an officer comes upon a container that might contain incriminating evidence, that container "may be opened immediately." *United States v. Ross*, 456

U.S. 798, 823 (1982).[8] The allowance of searching with immediacy suggests that the investigative team itself is allowed to search despite the possibility that innocuous materials might be present. Indeed, the Court stated that the privacy interest "must give way to *the prompt and efficient* completion of the task at hand." *Id.* at 821 (emphasis added).

Clearly, both the Supreme Court and the Eleventh Circuit have contemplated the realities of warranted searches. They both have carefully considered the Fourth Amendment protection that should be afforded to innocuous documents and found that searches must be allowed unimpeded despite the document owner's privacy interests. Accordingly, the Government will be afforded deference in determining the search protocol for the fruits of this warrant.

C. The Reasonableness of a Search Is Appropriately Judged After the Fact; Therefore, the Government Will Be Shown Deference in Executing the Search.

In the application for an arrest warrant, the Fourth Amendment interposes the "impartial judgment of a judicial officer" between citizens and the police "to assess the weight and credibility of the information which the complaining officer adduces as probable cause." *Wong Sun v. United States*, 371 U.S. 471, 481-482 (1963). The

[8] *Ross* concerns unwarranted searches of vehicles, but the Court stated that unwarranted searches of automobiles supported by probable cause should be given the same force a warranted search. Therefore, the reasoning applies to the current situation as well.

Supreme Court later clarified that this *ex ante* protection also applies to search warrants, adding that the Fourth Amendment provides, "*ex post*, a right to suppress evidence improperly obtained and a cause of action for damages." *Grubbs*, 547 U.S. at 99. That *ex post* protection is the "later judicial review as to [the] reasonableness" of a search that is required by *Dalia*. 441 U.S. at 258; *see supra* Part II at 7; *see also Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (*en banc*) (Noting that Fourth Amendment reasonableness is judged "after [factual] circumstances unfold, not before.").

Despite this guidance from the Supreme Court, magistrate judges have at times attempted to dictate the method that the Government should use to execute a warrant; however, district courts have found these attempts to be inappropriate. *In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp.3d 1 (D.D.C. 2014) (hereinafter "*Apple I*"). In *Apple I*, a magistrate judge feared that the search of an entire email account would be overly broad, so he refused to issue the warrant unless the Government agreed to use a filter team. *Id.* at 9. However, *Apple I* was reversed when it was reviewed by the district court. The district court reasoned that the Government's application for a warrant met the requirements set out in *Dalia* and, therefore, the court must issue the warrant without requiring a filter team. *In*

the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp.3d 157, 165. (D.D.C. 2014) (hereinafter "*Apple II*"). While the *Apple II* court found that the Government should be afforded deference in the execution of the search, it also reminded the Government that the search was subject to later review to determine whether it complied with the Fourth Amendment reasonableness requirement. *Id.* at 166.

A magistrate judge in the District of Kansas similarly denied a warrant application because the Government refused to use a filter team, despite there being no indication that privileged information was present. *In the Matter of the Search of Premises known as: Three Hotmail Email accounts: [redacted]@ hotmail.com, [redacted]@hotmail.com, [redacted] @hotmail.com Belonging to and Seized from [redacted].*, 2016 WL 1239916, at *24 (D. Kan. Mar. 28, 2016) (hereinafter "*Hotmail*"). The Government appealed the magistrate judge's determination to the district court. The district judge held that the filter team requirement was improper. *Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 2016 WL 5410401, at **10 (D. Kan. Sept. 28, 2016) (hereinafter "*Microsoft*"). The district court found that "so long as a warrant specifies with particularity what evidence the [G]overnment intends to seize, establishes probable cause that the evidence is connected to a specific criminal

statute, and includes some limitations (such as a date range) to prevent the potential of a general search, the warrant meets the Fourth Amendment particularity requirement." *Id.* The *Microsoft* court, like the *Apple II* court, found that the Government must be afforded discretion in how to execute its search. Therefore, the *Microsoft* court ruled, the court must issue the warrant without the filter team requirement. The court did, however, reiterate that the search itself is subject to later review to ensure it was reasonable.

Here, like in *Apple I* and *Hotmail*, the magistrate judge is concerned that the Government's intended search is so broad that it "eviscerates the particularity requirement." However, like the courts in *Apple II* and *Microsoft*, this court finds that probable cause has been shown to support the breadth of the search and that the particularity requirement has been satisfied. Therefore, the Government will be permitted to execute the search using the method it deems appropriate. Of course the search itself will be subject to later review as to its reasonableness.

IV. Conclusion and Orders

The Government's Motion To Review is **GRANTED**, and the Filter Team Order is **HEREBY VACATED**.

DONE and **ORDERED** this 8th day of August, 2017.

VIRGINIA EMERSON HOPKINS
United States District Judge